UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,029	08/14/2001	William B. Sweet	055120-0002	3170

7590 09/08/2005

William Sweet
2665 North First St
Suite 300
San Jose, CA 95134

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 09/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

4

Office Action Summary	**Application No.** 09/930,029	**Applicant(s)** SWEET ET AL.
	Examiner Jeffrey D. Popham	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 52-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-58* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *see continuation*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

4

IDSs:
20010814, 20020819, 20030417

Remarks

Claims 1-22 and 52-58 are pending.

Claim Objections

1. Claims 7, 13, 16, 57, and 58 are objected to because of the following informalities:

- Claim 7, part (f) reads "authorizing the user". There is insufficient antecedent basis for this limitation in the claim. For purposes of prior art rejection, it has been construed as "authorizing a user".
- Claim 13 recites the limitation "the access permission security profile". There is insufficient antecedent basis for this limitation in the claims. For purposes of prior art rejection, claim 13 has been construed as being dependent upon claim 10.
- Claim 16 is a multiple dependent claim, and one of these claims that it is dependent upon is claim 11. Within claim 11, there is insufficient antecedent basis for "the access permission security profile". For purposes of prior art rejection, claim 16 has been construed as being dependent upon claims 1, 4, 9, and 10 only.
- Claims 57 and 58 read "the method of claim 1, 4, 7, 23, 32, 46, or 52". Since claims 23-52 have been cancelled, they has been construed as being dependent upon claims 1, 4, 7, or 52. Also, seeing as claim 52 is a system

claim, the preamble to claims 57 and 58 should read “the method or system of claim 1, 4, 7, or 52”.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-20, and 52-57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt (U.S. Patent 6,490,680) in view of Shwartz (Shwartz, John, “Techway; For a Switch, the Code Knows You; A Vienna Firm Is Offering a High-Tech Twist: Selective Encryption”, The Washington Post (F.05), 11/1/1999, pp. 1-3).

Regarding Claim 1,

Scheidt discloses a method for providing cryptographic capabilities to a plurality of network users, comprising:

(a) receiving a request for an access permission security profile on behalf of a network user (Column 14, lines 30-45);

(b) authenticating the request (Column 14, lines 30-45);

(c) creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object (Column 9, lines 31-38);

(d) securely transmitting the access permission security profile to the network user over the network (Column 14, lines 30-45).

Scheidt does not disclose that this is done on a decentralized public network.

Shwartz, however, discloses that this is done on a decentralized public network (Page 2, Paragraphs 2-8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the cryptography system of Shwartz into the access control system of Scheidt in order to perform the brunt of the processing on the user's machine, thus lowering the burden on the servers, and to display web pages on the user's machine that do not look edited, so the user sees no remnants of information that he does not have access to (by the web page not being formatted correctly, etc.).

Regarding Claim 2,

Scheidt discloses that the creating step comprises:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 16, lines 11-27);

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 8, lines 31-44; and Column 9, lines 31-38); and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 9, lines 31-38).

Regarding Claim 3,

Scheidt discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 8, lines 18-44; and Column 9, lines 31-38).

Regarding Claim 4,

Scheidt discloses a method for providing decryption capabilities to a plurality of network users, comprising:

(a) receiving a request for decryption capabilities on behalf of a network user (Column 14, lines 30-45);

(b) authenticating the request (Column 14, lines 30-45);

(c) creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object (Column 9, lines 31-38);

(d) receiving from the user information associated with the encrypted object (Column 17, lines 15-34);

(e) generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object (Column 17, lines 15-34); and

(f) securely transmitting the cryptographic key to the network user over the network (Column 17, lines 15-34).

Scheidt does not disclose that this is done on a decentralized public network.

Shwartz, however, discloses that this is done on a decentralized public network (Page 2, Paragraphs 2-8).

Regarding Claim 5,

Scheidt discloses that the creating step includes:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 16, lines 11-27);

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 8, lines 31-44; and Column 9, lines 31-38); and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 9, lines 31-38).

Regarding Claim 6,

Scheidt discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 8, lines 18-44; and Column 9, lines 31-38).

Regarding Claim 7,

Scheidt discloses a method for cryptographically securing the distribution of information to a plurality of network users, comprising:

(a) creating a computer representable data object including one or more embedded objects (Column 16, lines 11 to 27);

(b) selecting one or more embedded objects of the data object (data separation) to be encrypted (Column 16, lines 11-27);

(c) encrypting the selected embedded objects (Column 16, lines 11-27);

(d) creating one or more access permission credentials (Column 16, lines 28-33);

(e) assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object (Column 16, lines 28-33);

(f) authorizing a user (Column 14, lines 30-38; and Column 17, lines 16-36);

(g) transmitting the data object over the network (Column 14, lines 16-22).

Scheidt does not disclose that this is done on a decentralized public network.

Shwartz, however, discloses that this is done on a decentralized public network (Page 2, Paragraphs 2-8).

Regarding Claim 8,

Scheidt discloses that the information is digital content (Column 7, lines 12-27).

Regarding Claim 9,

Scheidt discloses that the authorizing step includes:

(i) receiving a request for an access permission security profile on behalf of a network user (Column 14, lines 30-45);

(ii) authenticating the request (Column 14, lines 30-45); and

(iii) securely transmitting the security profile to the network user over the network (Column 14, lines 30-45).

Regarding Claim 10,

Scheidt discloses that the authorizing step includes:

(i) sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network (Column 14, lines 30-45);

(ii) receiving the request at the central server system (Column 14, lines 30-45);

(iii) authenticating the request (Column 14, lines 30-45); and

(iv) securely transmitting the security profile from the server system to the network user over the network (Column 14, lines 30-45).

Regarding Claim 11,

Scheidt discloses that the authorizing step is automatic and based upon the user's possession of a security profile token (Column 11, lines 22-30).

Regarding Claim 12,

Scheidt discloses that the encrypting step comprises:

(i) identifying a group of network users who are to be allowed access to a data object to be encrypted (Column 16, lines 11 to 27);

(ii) generating an appropriate cryptographic credential key from a set of credential categories, the credential key relating to the group of network users (Column 10, line 53 to Column 11, line 12);

(iii) generating a cryptographic working key from at least a domain component, a maintenance component, and a pseudorandom component (Column 10, line 53 to Column 11, line 12);

(iv) encrypting the data object with the working key (Column 16, lines 11-27);

(v) encrypting the pseudorandom component with the credential key (Column 16, line 34 to Column 17, line 8); and

(vi) associating the encrypted pseudorandom component to the encrypted data object (in the header) (Column 16, line 34 to Column 17, line 8).

Regarding Claim 13,

Scheidt discloses that the access permission security profile is created by:

(i) identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 16, lines 11-27);

(ii) establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 8, lines 31-44; and Column 9, lines 31-38); and

(iii) creating one or more security profiles for each network user, wherein each security profile contains at least one access code (Column 9, lines 31-38).

Regarding Claim 14,

Scheidt discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 8, lines 18-44; and Column 9, lines 31-38).

Regarding Claim 15,

Scheidt discloses that the request is initiated in-band by the network user over the network (Column 14, lines 30-45).

Regarding Claim 16,

Scheidt discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 8, lines 46-62).

Regarding Claim 17,

Scheidt discloses that the authenticating step includes the use of biometric information (Column 12, line 46 to Column 13, line 19).

Regarding Claim 18,

Scheidt discloses that the authenticating step includes the use of a hardware token (Column 11, lines 22 to 30; and Column 11, line 65 to Column 12, line 46).

Regarding Claim 19,

Scheidt discloses that the authenticating step includes the use of a software token (Column 14, lines 30-45).

Regarding Claim 20,

Scheidt discloses that the authenticating step includes the use of a user password (Column 11, lines 14-20).

Regarding Claim 52,

Scheidt discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a network, comprising:

(a) a plurality of member tokens for providing cryptographic capabilities to authenticated users of the network (Column 9, lines 31-48);

(b) a set of server systems for managing the distribution of the member tokens (Column 7, lines 13-58);

(c) means for requesting a member token from at least one server system (Column 9, lines 24-38; and Figure 6);

(d) a set of client systems, wherein each client system includes

(i) means for receiving the requested member token (Column 10, lines 19-25), and

(ii) means for utilizing the cryptographic capabilities provided by the member token (Column 14, lines 30-45); and

(e) means for securely distributing a requested member token from at least one server system to at least one client system over the network (Column 10, lines 19-25).

Scheidt does not disclose that the network is a decentralized public network.

Shwartz, however, discloses that the network is a decentralized public network (Page 2, Paragraphs 2-8).

Regarding Claim 53,

Scheidt discloses that each client system further includes user authentication means (Column 11, lines 14-40).

Regarding Claim 54,

Scheidt discloses that the means for requesting a member token resides on each client system (Column 9, lines 24-38; and Figure 6).

Regarding Claim 55,

Scheidt discloses that means for authenticating a user resides on at least one server system (Column 7, lines 13-58; and Column 13, lines 22-36).

Regarding Claim 56,

Scheidt discloses that managing the distribution of the member tokens includes updating of the member tokens (Column 10, lines 14-25).

Regarding Claim 57,

Shwartz discloses that the decentralized public network is the Internet (Page 2, Paragraphs 2-8).

3. Claims 21, 22, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Scheidt in view of Shwartz, further in view of Anderson (U.S. Patent 5,805,674).

Regarding Claim 21,

Scheidt as modified by Shwartz does not disclose that the authenticating step includes the use of a record time at which the request was made.

Anderson, however, discloses that the authenticating step includes the use of a record of time at which the request was made (Column 11, line 62 to Column 12, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the cell phone security system of Anderson into the access control system of Scheidt as modified by Shwartz in order to allow the system to increase a level of authentication (such as, by requiring biometrics where a password is normally sufficient) in response to suspicious events.

Regarding Claim 22,

Anderson discloses that the authenticating step includes the use of a record of the user's physical location (Column 11, lines 29-34).

Regarding Claim 58,

Anderson discloses that the decentralized public network is a cellular phone network (Column 4, lines 21-33).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E. Moise
EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER